REMARKS

Claims 1 – 3, 5, 7-9, 12-17, and 19-29 are currently pending in the application. All pending claims are presented for reconsideration and reexamination in view of the following remarks.

In the outstanding Office Action, claims 1-3, 5, 7-9, 12-17 and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,732,278 to Baird, III et al. (hereafter, "Baird") in view of U.S. Patent No. 6,720,861 to Rodenbeck et al. (hereafter, "Rodenbeck"); and claims 20-29 were further rejected under 35 U.S.C. § 103(a) as being unpatentable over Baird in view of U.S. Patent Application Publication No. 2002/0104006 A1 to Boate et al. (hereafter, "Boate") and in further view of Rodenbeck.

By this Response, the Examiner's rejections have been traversed.

Rejection under 35 U.S.C. § 103(a)

1. Rejection of claims 1-3, 5, 7-9, 12-17, and 19.

The Examiner rejected claims 1-3, 5, 7-9, 12-17, and 19 as being unpatentable over Baird in view of Rodenbeck.

Response

Reconsideration and withdrawal of the rejection are respectfully requested.

To establish a *prima facie* case of obviousness, the Examiner must establish: (1) that some suggestion or motivation to modify the references exists; (2) a reasonable expectation of success; and (3) that the prior art references teach or suggest all the claim limitations. Amgen, Inc. v. Chugai Pharm. Co., 18 USPQ2d 1016, 1023 (Fed. Cir. 1991); In re Fine, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988); In re Wilson, 165 USPQ 494, 496 (C.C.P.A. 1970).

It is respectfully submitted that the combination of references fails to teach or suggest all the claim limitations. By this Response, the rejections to independent claims 1 and 12, and to the claims dependent upon claims 1 and 12, are respectfully traversed.

Independent claims 1 and 12 recite, *inter alia*, "triggering a user status change upon valid entry or exit through a door of a building."

Baird teaches a security method wherein a user is granted access to an informational asset by authenticating the user through one or more of a user password, a biometric measure, and a computer-generated password. See Summary of the Invention. The Examiner states that "Baird does not explicitly teach triggering a user status change upon valid entry or exit through a *door of a building*. However, Rodenbeck discloses triggering a user status change upon valid entry or exit through a door of a building." See Office Action at page 3.

Rodenbeck teaches an access control system wherein a user is granted access to a physical asset by a remote access control system (RACS). The RACS communicates bidirectionally with a central access control system (CACS) to determine whether the user is to be granted access to the physical asset. See column 4, lines 45 to 55.

The combination of Baird and Rodenbeck fails to disclose, teach, or suggest the feature of "*triggering* a user status change upon valid entry or exit through a door of a building" as recited in independent claims 1 and 12 (emphasis added). It is argued in the Office Action that Rodenbeck discloses this feature as recited in the claims. However, communication between the RACS and the CACS in Rodenbeck's design is periodic. See, for example, Rodenbeck column 4, lines 48-55 which reads: "remote access controller 62 can send or receive information to or from central access controller 30...This allows remote access controller 62 to send *periodic* user access information to central access controller” (*emphasis added).* Rodenbeck does not disclose, teach, or suggest that the communication between the door and a central access occurs as a trigger with an entry or exit event. In contrast, claims 1 and 12 of the present application state that valid entry or exit through the door of a building will trigger a user status change; such a trigger does not rely on periodic communication, but rather on communication that occurs with an entry or exit event.

Moreover, Rodenbeck teaches that communication from the RACS to the CACS is for tracking and monitoring purposes. See, for example, Rodenbeck column 3, lines 36-40 which reads: “The central access control system 20 can also receive information from each remote access control system 22 so that user access information *such as the time and date that a particular user 12 was granted access through door 14 can be tracked and monitored*” (emphasis added). See also Rodenbeck col. 5 lines 21-29 which reads: “Information can also be communicated wirelessly form the remote access controller 62 to central access control system 20...This type of wireless communication allows user access information *to be monitored and tracked...*” (emphasis added).

In contrast, the present application teaches that entry and exit events are communicated to the Security Access Service Provider (“SASP”) for physical asset protection and information asset protection (see the present application, preamble of claims 1 and 12); the information communicated to the SASP can be used for physical intrusion monitoring, physical access control, network access control, secure asset tracking, employee tracking, and visitor tracking (see Specifications page 14). Rodenbeck does not disclose, teach, or suggest that the amount and type of information communicated between the remote access controller and the central access controller is sufficient for these purposes, or for those described throughout the specification of the present invention.

Claim 1 further recites, *inter alia*, "*transmitting a breach* of physical asset protection in the hosted environment such that information asset protection is maintained by denying access thereto" (emphasis added). Claim 12 recites, *inter alia,* "denying access to the information asset in the hosted environment *when there is a breach* of the physical asset protection" (emphasis added). Rodenbeck teaches an access control system in which the RACS queries the CACS for a given user's authorization. See column 8, line 47 to column 9, line 5. Rodenbeck fails to disclose, teach, or suggest that the RACS would or could transmit a breach of door protection to the CACS. One significant advantage of the present invention is the ability for the SASP to control access to physical and information assets on the basis of not only valid entry and exit events, but also invalid attempts at entry or exit. See page 12, paragraph 2 of the specification, where "[i]f a user attempts to gain physical access to a door without valid credentials, then the denied entry attempt is logged in the physical access database"; see also page 9, paragraph 3 of the specification, where "information system access can be denied based on an employee...being denied physical access."

Thus the security control system of Rodenbeck, even in combination with that of Baird, would not suggest a system where a physical or information asset is protected by triggering a user status change upon valid entry or exit through a door of a building. Further, the security control system of Rodenbeck, even in combination with that of Baird, would not suggest a system which transmits a breach of physical asset protection in the hosted environment such that information asset protection is maintained by denying access thereto.

As claims 2-3, 5, and 7-9 are dependent on independent claim 1, which is believed to be allowable, Applicant respectfully submits that these claims are also allowable for at least the same reasons as claim 1.

As claims 13-17 and 19 are dependent on independent claim 12, which is believed to be allowable, Applicant respectfully submits that these claims are also allowable for at least the same reasons as claim 12.

2. Rejection of claims 20-29

The Examiner rejected claims 20-29 as being unpatentable over Baird in view of Boate and Rodenbeck.

Response

Reconsideration and withdrawal of the rejection are respectfully requested.

It is respectfully submitted that the combination of references fails to teach or suggest all the claim limitations. By this Response, the rejections to independent claim 20, and to the claims dependent upon claims 20, are respectfully traversed.

Independent claim 20 recites, *inter alia*, that "a user status change is triggered upon valid entry or exit through a door of a building."

All descriptions of Baird and Rodenbeck above are incorporated herein by reference. Baird teaches a method of asset protection in which access is granted after an authentication process. Even *assuming arguendo* that Boate teaches transmitting and receiving a signal to a host environment, the reference fails to cure the deficiency of Baird, namely, triggering a user status change upon valid entry or exit through a *door of a building.* As the Examiner notes in the pending Office Action, "Baird and Boate do not explicitly teach triggering a user status change upon valid entry or exit through the door of a building." See Office Action at page 9.

The combination of Baird, Boate, and Rodenbeck fail to disclose, teach, or suggest the feature of "a user status change" that is "*triggered* upon valid entry or exit through a door of a building" (emphasis added). It is argued in the Office Action that Rodenbeck discloses this feature as recited in the claims. However, Rodenbeck does not disclose, teach, or suggest that the communication between the door and a central access occurs as a trigger with an entry or exit event. Moreover, Rodenbeck does not disclose, teach, or suggest that the information communicated between the remote access controller and the central access controller is sufficient for the purpose of communicating an entry or exit event, or for those purposes described throughout the specification of the present invention. Thus, the security control system of Rodenbeck, even in combination with that of Baird and Boate, would not suggest a system where a physical or information asset is protected by triggering a user status change upon valid entry or exit through a door of a building.

Claim 20 further recites, *inter alia*, "receiving a second signal from said hosted environment indicative of asset access." Baird, Rodenbeck, and Boate all teach signals sent from the host environment that confirm authenticity. Baird, Rodenbeck, and Boate do not teach signals sent from the host environment indicative of asset access. As described above, in the present invention the SASP can control access to physical and information assets on the basis of not only valid entry and exit events, but also invalid attempts at entry or exit. All entry and exit events, including invalid attempts, are communications from the hosted environment indicative of asset access, which are capable of, but are not limited to, informing the recipient of a "user status change" (see claim 20) such as a breach of access.

Thus the security control systems of Rodenbeck, even in combination with those of Baird and Boate, would not suggest a system which transmits information about asset access from a hosted environment wherein protection of physical and information characteristics of said asset is integrated in said hosted environment, as recited in claim 20.

As claims 21-29 are dependent on independent claim 20, which is believed to be allowable, Applicant respectfully submits that these claims are also allowable for at least the same reasons as claim 20.

CONCLUSION

In light of the foregoing, Applicant submits that the application is now in condition for allowance. If the Examiner believes the application is not in condition for allowance, Applicant respectfully requests that the Examiner contact the undersigned attorney if it is believed that such contact will expedite the prosecution of the application.

In the event this paper is not timely filed, Applicant petitions for an appropriate extension of time. Please charge any fee deficiency or credit any overpayment to Deposit Account No. 14-0112. Favorable action with an early allowance of the claims is earnestly solicited.

Respectfully submitted,

NATH & ASSOCIATES PLLC

October 5, 2005

NATH & ASSOCIATES PLLC
1030 15th Street, N.W.
6th Floor
Washington, D.C. 20005
Tel: (202) 775-8383
Fax: (202) 775-8396

Gary M. Nath
Reg. No. 26,965
Gregory B. Kang
Reg. No. 45,273
Teresa M. Arroyo
Reg. No. 50,015
Customer No. 20529